UNITED STATES DISTRICT COURT

for the

District of New Jersey

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The Loews Hotel,1200 Market Street, Philadelphia, Pennsylvania 19107, room 2411, as more fully described in Attachment A-2

Case No. 20- 375

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-2

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1349	Conspiracy to commit bank fraud and wire fraud.

The application is based on these facts:

See Attachment C

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kristin Savoy, Special Agent, H.S.I.
Printed name and title

Sworn to before me and signed in my presence.

Date: 02/12/2020

Judge's signature

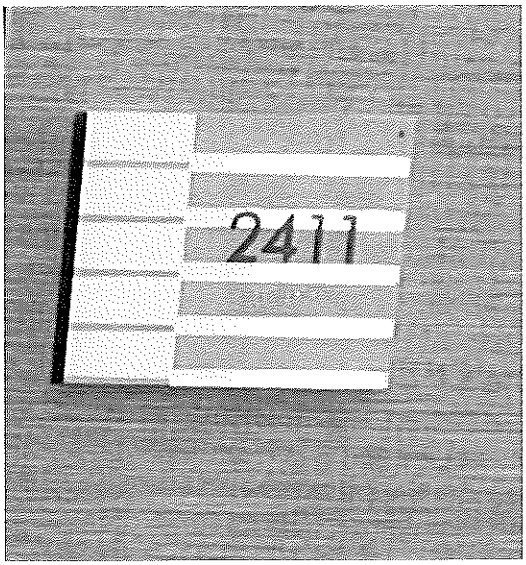
City and state: Philadelphia, Pennsylvania

Jacob Hart, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-2

Property to Be Searched

Hotel room 2411 is located in the Loews Hotel located at 1200 Market Street, Philadelphia, Pennsylvania 19107, the premises to be searched is a hotel room (hereinafter referred to as "SUBJECT PREMISES B") with a black door containing a plaque numbered 2411 to the right of the door. SUBJECT PREMISES B is located on the twenty fourth floor of the hotel. SUBJECT PREMISES B is also depicted in the attached photograph.



ATTACHMENT B-2

Particular Things to be Seized

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1349; conspiracy to commit wire fraud, contrary to Title 18 U.S.C. § 1343, and bank fraud contrary to Title 18 U.S.C. § 1344, namely:

1. Electronic equipment (including searching the memory and contents thereof), such as computers, computer hardware, printers, cellular telephones (including smart phones), tablets and external hard drive ("devices") and storage media. Additionally, computer software and the contents therein, containing the information generated by the aforementioned electronic equipment. Further, any recording equipment and security equipment used to monitor and record activities;
2. United States currency, rare coins, currency counting machines, precious metals, designer clothing and accessories, designer shoes, jewelry, and financial instruments, including stocks and bonds, representing bank fraud, money laundering and identity theft in an amount or with a value in excess of approximately $500;
3. Photographs, records and documents, and any video, recording or photographic equipment containing the aforementioned items, containing information regarding the identities of coconspirators or those involved in money laundering;
4. Address and/or telephone books, Rolodex indices, and any papers or records reflecting names, addresses, telephone numbers, pager numbers, facsimile numbers and/or telex numbers of co-conspirators, financial institutions, and other individuals or businesses with whom a financial relationship exists;
5. Indicia of occupancy, residency, and ownership or use of the subject premises, including but not limited to, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, and keys;

6. Reports, records or any other document or item relating or referring to official or unofficial law enforcement activities and investigations relating to bank fraud, money laundering and identity theft;
7. General journals, cash receipt journals, cash disbursement journals, sales journals and computer printout sheets, check making materials including blank check stock, printers, and ink cartridges;
8. General ledgers and subsidiary ledgers including notes receivables, accounts receivables, accounts payable, notes payable, adjusting journals and closing ledgers;
9. All bank deposit slips, withdrawal slips and any and all checks to include cancelled checks for any and all accounts, including all funds on deposit such as certificates of deposit, money market accounts, negotiable order of withdrawal accounts (NOW), ATM/debit cards, code numbers or related records of deposits and withdrawals, wire transfer application and advises, bank bags, and bank safety deposit box records and keys;
10. Credit cards, prepaid credit cards and re-loadable cards, and financial statements relating to them;
11. Receipts and invoices for all expenditures relating to money laundering activities;
12. All Federal income tax returns, Forms 1040, W-2, 1099, 1120, 940, 941, K-1, or copies of same and supporting work papers, summary sheets, and analyses used in the preparation of the tax returns;
13. All financial statements or other documentation supporting conveyances and/or ownership of properties, and vehicle documentation to include registration, tag and titles;
14. All documents relating to communications involving the Target Subjects during which constitute fruits, evidence and/or instrumentalities of violations of Title 18, United States Code, Section 1956;

15. Any safes, locked cabinets, and/or other secured containers and/or devices at the location described in Attachment A-2 that contain any of the items set forth in Attachment B-2. Law enforcement shall be permitted to open such locked containers by force or through the use of a locksmith if necessary.

ATTACHMENT C

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH AND SEIZURE WARRANT FOR SUBJECT PREMISES A AND SUBJECT PREMISES B

I, Kristin Savoy, being duly sworn, do hereby state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations ("HSI"), assigned to the Cherry Hill, New Jersey Resident Agent in Charge Office. I have been employed as a special agent for twenty-three years. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, U.S.C. § 2501(7), that is an officer of the United States who is empowered by law to conduct investigations of, and make arrests for, offenses against the United States.

2. I have successfully completed the Criminal Investigator Training Program ("CITP") and the ICE Special Agent Training Program ("ICESAT") at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, and have experience in the investigation and prosecution of violations of firearms violations, narcotics, money laundering, fraud, violent crimes and other federal criminal laws. I have previously executed and participated in the execution of numerous search warrants for violations of federal laws.

3. I am familiar with the facts and circumstances set forth herein through my personal participation in this investigation and based on information provided by other law enforcement officers not limited to Homeland Security Investigations (HSI), the United States Marshal Service(USML), the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF"), Glassboro Police Department, Glassboro, New Jersey, Winslow Police Department, Winslow, New Jersey and the New Jersey State Police, all of which are also involved in this investigation. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact known to me from this investigation.

4. This Affidavit is submitted in support of an application under Fed. R. Crim. P. 41 for a search and seizure warrant for hotel rooms 2208 (hereinafter "SUBJECT PREMISES A") and 2411 (hereinafter "SUBJECT PREMISES B") located within the Loews Hotel, located at 1200 Market Street, Philadelphia, Pennsylvania 19107 (hereinafter collectively the "SUBJECT PREMISES"), for evidence, instrumentalities, contraband, and fruits of the crime of conspiracy to commit wire fraud contrary to Title 18, United States Code, Section 1343 and bank fraud contrary to Title 18 U.S.C. § 1344, in violation of Title 18, United States Code, Section 1349 (hereinafter the "Specified Federal Offenses"). For the reasons set forth below, I have probable cause to believe there is evidence at that location related to the TARGET OFFENSES.

5. This affidavit is being submitted in support of an Application for Search Warrant for SUBJECT PREMISES A, as more fully described in Attachment A-1 as follows: A hotel room within the Loews Hotel identified as hotel room number 2208. The hotel room door is black in color and there is a room plaque on the right hand side of the door with the numbers "2208" clearly marked. Based upon the information set forth herein, there is probable cause to believe, the SUBJECT PREMISES will contain evidence, fruits, and instrumentalities of the Specified Federal Offenses, as set forth in Attachment B-2.

6. This affidavit is being submitted in support of an Application for Search Warrant for SUBJECT PREMISES B, as more fully described in Attachment A-1 as follows: A hotel room within the Loews Hotel identified as hotel room number 2411. The hotel room door is black in color and there is a room plaque on the right hand side of the door with the numbers "2411" clearly marked.

REVELANT SECTIONS OF LAW

7. Based upon my training and experience, I am familiar with the Specified Federal Offenses and other related crimes including money laundering, in violation of Title 18 U.S.C § 1956, and conspiracy to defraud the United States, in violation of 18 U.S.C. § 371.

PROBABLE CAUSE

8. Based upon my training, experience, and discussions with other law enforcement members related to the investigation of fraud scheme, I am aware that on February 7, 2020, Federal arrest warrants were sworn out for Kayla MASSA (hereinafter "MASSA"), William LOGAN (hereinafter "LOGAN") and Jabreel MARTIN (hereinafter "MARTIN") (collectively the "Target Subjects") in the United States Magistrate Court for the District of New Jersey, in Camden, before the Honorable U.S. Magistrate Judge Karen M. Williams for knowingly and intentionally conspiring and agreeing with others, known and unknown, to devise a scheme and artifice to defraud financial institutions and the United States, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice: (1) to cause to be transmitted by means of wire communications in interstate and foreign commerce, certain signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343; (2) to defraud a financial institution by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344, in violation of Title 18, United States Code Section 1349 (hereinafter the "Specified Federal Offenses").

9. On February 11, 2020, investigators learned information indicating LOGAN was currently staying at the Lowes Hotel. Further investigations confirmed that LOGAN was currently a registered guest to the "SUBJECT PREMISES A." LOGAN's room reservation was booked under the name Jacob Carter. The reservation was paid in cash and had a scheduled checkout date of February 12, 2020.

10. On February 11, 2020, investigators learned information indicating MASSA was also currently staying at the Lowes Hotel. Further investigations confirmed that MASSA was a registered guest to the "SUBJECT PREMISES B." MASSA's room reservation was made with a credit card

through an internet hotel booking website under the name Amanda Allison, which is believed to be LOGAN's mother's name. No one named Amanda Allison was identified at the location. The reservation had a scheduled checkout date of February 12, 2020.

11. Law enforcement agents obtained video posted by a male who was with LOGAN on the evening of February 11, 2020, filmed inside a room in the Lowes Hotel, brandishing two individual handguns, both appearing to be semi-automatic pistols. LOGAN can be heard speaking in the background of the video. The video was posted "live" from the room on an Instagram account.

12. SUBJECT PREMISES A is located on the 22nd floor of the Lowes Hotel, and SUBJECT PREMISES B is located on the 24th floor of the Lowes Hotel.

13. On February 12, 2020 investigators identified confirmed MARTIN was at the Lowes Hotel with LOGAN and MASSA. MARTIN was identified through live surveillance footage coming and going between SUBJECT PREMISES A and SUBJECT PREMISES B.

14. Law enforcement agents confirmed through physical surveillance that LOGAN and MASSA were on-site at the "SUBJECT PREMISES" during the evening of February 11, 2020. On February 12, 2020 physical surveillance was re-initiated at the "SUBJECT PREMISES." Law enforcement agents established physical surveillance in close proximity to SUBJECT PREMISES A and SUBJECT PREMISES B along with ongoing coverage of live surveillance footage that was maintained by the Lowes Hotel. During the course of surveillance, LOGAN, MARTIN, and an unidentified male were observed coming and going between SUBJECT PREMISES A and SUBJECT PREMISES B, and not stopping in any other rooms. At or around 10:30 a.m., law enforcement agents saw MARTIN walk alone from room SUBJECT PREMISES A to SUBJECT PREMISES B. At or around 11:15 a.m., law enforcement agents observed MARTIN exit SUBJECT PREMISES A, enter the elevator, and exit the

elevator at the lobby level on the first floor. Upon exiting the elevator, MARTIN was taken into custody. MARTIN was patted down for agent safety and no weapons were recovered.

15. At or around 11:30 a.m., law enforcement officers made contact with MASSA in SUBJECT PREMISES B. Upon entry to the room MASSA was identified and secured. During a protective sweep of the hotel room, one 9mm semi-automatic handgun was observed in plain view on a blue chair within the hotel room. Law enforcement officers also discovered items consistent with being used in the commission of the Specified Federal Offenses on a table located inside the room. Those items include a laptop computer, a printer, stacks of blank checks, and several newly printed counterfeit checks. I know these items are commonly used to commit the Specified Federal Offenses. I am not aware that MASSA or LOGAN have a valid license to carry a firearm in the State of Pennsylvania.

16. Based on the items observed by law enforcement agents in the SUBJECT PREMISES, and recovery of only one of two handguns believed to be in possession of LOGAN and MASSA, I believe that the SUBJECT PREMISES A and SUBJECT PREMISES B and will contain further evidence, fruits, and instrumentalities of the Specified Federal Offenses. Accordingly, at this time, probable cause exists to search SUBJECT PREMISES A and SUBJECT PREMISES B and seize evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses, as further described in Attachment B-1 and Attachment B-2.

PHYSICAL EVIDENCE, ELECTRONIC EVIDENCE, TELEPHONES, COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B-1 and B-2, this application seeks permission to search for records that might be found in SUBJECT PREMISES A and SUBJECT PREMISES B, in whatever form they are found. One form in which the records might be found is as data stored on a computer's hard drive or other storage media (including cellular telephones). Thus, the warrant applied for would authorize the copying of electronically stored information, all under Rule 41(e)(2)(B). Those

involved in financial crimes, including bank fraud, often conceal stolen checks, credit cards, debit cards, stored value cards, money orders, fraudulent identification documents, financial documents, account information, and account ledgers with their residences, and in bank safe deposit boxes, automobiles, businesses, and storage facilities. These items are stored in such areas for ready access and to conceal them from law enforcement. I also know that individuals who commit multiple acts of bank fraud typically maintain documents related to those offenses for months and even years, in order to facilitate further fraud and theft.

18. Based on my training and experience, I believe that individuals who engage in bank fraud will often use bank fraud to engage in financial fraud in order to gain access to US Currency, credit cards, debit cards, and stored value cards. These individuals will then use the credit, debit, and stored value cards to conduct purchases, cash advances, ATM withdrawals, and other financial transactions. Individuals will often use their personal vehicle to travel to numerous bank branches, ATM terminals, and merchants to conduct this activity. Commonly, receipts are generated from these financial transactions and purchases and retained, and they are often inadvertently left in a vehicle.

19. Based on my training and experience, I know that individuals who engage in money laundering, bank fraud, and other financial crimes keep fruits of this criminal activity in the form of cash, jewelry, expensive shoes, expensive clothing, cars, electronic equipment, and other luxury items that they believe keep their value. I know that individuals who use proceeds of criminal activity to purchase luxury items will keep the luxury items with them at their residence or at a location where they are residing. Individuals do this because they want to keep the luxury items from being stolen, misplaced, or lost. Based on my training and experience, I know that even when individuals move to different residences, they will take these luxury items and any other fruits of their illegal activity with them to the new residences. Based on my training and experience, and in the context of this case, I

believe that individuals engaged in the type of fraud described in this affidavit will often use the proceeds of the fraud to purchase luxury goods for themselves and their loved ones in an attempt to conceal the source of funds that were used to purchase the items. In such cases, I believe those individuals believe that purchasing the luxury goods with the unlawfully gained funds will hide the funds from law enforcement agents. I also believe that the individuals believe that the luxury items purchased will maintain their own value over time, thus further obscuring the illegal nature of the funds.

20. Based on my training and experience, I believe that individuals who engage in bank fraud and document counterfeiting commonly use computers, scanners, color printers, digital cameras, and graphic design software to help facilitate their scheme. These items are used to scan, create, alter, modify, adjust, and falsify documents, both original and counterfeit, to the needs of the individual and the accomplices. Individuals commonly use such devices to create, alter, modify, adjust, and falsify items such as identification cards, driver's licenses, checks, government documents, birth certificates, social security cards, tax forms, and business, government, or personal letterheads. In addition to the traditional uses of computer equipment listed above, individuals engaged in bank fraud commonly obtain information regarding their fraudulent identities from commercial and public source databases that are readily available on the Internet.

21. Based on my training and experience, I believe that individuals who engage in bank fraud often keep their computers and computer related equipment at their residences and in personally owned vehicles. Individuals engaged in bank fraud and related crimes will often use cellular telephones to check the status of purchases, accounts balances, and account transactions, as well as checking email with the Internet connections which modern smart phones allow. These individuals will also use their cellular telephones to communicate with co-conspirators. The communications will often include correspondence via voice calls, voice mail, text messages, SMS messages, MMS messages, e-mails,

social media messages and posts, and messages shared via "chat" or other third party messaging applications.

22. Based on my training and experience, and in the context of this investigation, individuals conduct a considerable amount of communication using their cellular telephones. Those communications are in the form of voice calls, text messages, SMS messages, MMS messages, e-mails, social media messages and posts, and messages shared via "chat" applications.

23. I know that individuals often utilize their cellular phones and smartphones to access the Internet and that each time this is done the device maintains a record or "browser history," showing which websites were visited and when. Investigators have confirmed that during the course of the investigation MASSA and LOGAN and co-conspirators utilized cellular phones to post advertisements in furtherance of the fraud scheme, communicated with victims via various messaging apps, conducted mobile deposits, and utilized cellular phones to retrieve victim's identity/ bank log in credentials routinely. I believe that MASSA and LOGAN likely accessed the internet via cellular phones.

24. I know through training and experience smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

25. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and digital tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Bank Fraud and identity theft can therefore be easily,

inexpensively and anonymously (through electronic communications) conducted by anyone with access to a computer or smartphone.

26. Individuals also use online resources to retrieve and store data to include photos and application data from their mobile devices. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of bank fraud and identity theft can be found on the user's computer, smartphone or external media in most cases.

27. I know through training and experience, as well as through consultation with a trained cellular phone forensic examiner, that evidence of the above forms of communication, and the browser history of such devices, are often kept in cell phones for months and even years. I know that a forensic examiner may be able to recover messages and other data that were manually deleted by the user of the phone. I know that persons who have cell phones often keep outdated or older models of phones they once used. I know that electronic data can be downloaded or copied in multiple devices at the same time. I also know that electronic data can be migrated between similar devices such a cellular phones, as well as between different devices such as cellular phones and laptops. For these reasons, I believe that any cellular phones and smartphones utilized by MASSA and LOGAN will contain communications with victims, banking details related to fraud and Instagram stories and images documenting said fraud. For all of these reasons, I request authorization to seize and search any cellular phones or smartphones found on the premises that is associated with MASSA, LOGAN, and MARTIN. The cellular telephones that will be seized will have a direct connection to MASSA, LOGAN, and MARTIN.

SEIZURE AND SEARCH OF DIGITAL DATA

28. Probable cause as to digital data: I submit that if a computer, cellular device, or storage medium is found in the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

i. Because this investigation involves bank fraud committed through the use of social media advertising, mobile messaging and mobile banking it is very likely that a computer or cellular device was used to facilitate the fraud, and there may be a computer system or cellular device located in the SUBJECT PREMISES.

ii. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

iii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

iv. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

v. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. Forensic evidence concerning digital data: As further described in Attachment B-1, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to

believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

v. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

vi. I know that when an individual uses a computer/cellular phone to commit fraud, it is an instrumentality and also a storage medium for evidence of the crime. The computer/cellular phone is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer/cellular phone is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that a computer/cellular used to commit a crime of this type may contain: data that is evidence of how the computer/cellular phone was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

30. Ability to copy entire computers or storage media: Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted

files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the location could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the location. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

iii. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit imaging or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

32. Based upon the above facts, I have probable cause to believe that SUBJECT PREMISES A and SUBJECT PREMISES B, as further described in Attachment A-1 and Attachment A-2, will contain evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses, as further described in Attachment B-1 and Attachment B-2. Therefore, I respectfully request that the Court issue a warrant to search SUBJECT PREMISES A and SUBJECT PREMISES B during normal, hours.

33. I further request that the Court order that all papers in support of this application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Kristin Savoy
Special Agent
Department of Homeland Security

Subscribed and sworn to before me
this 12 Day of February, 2020:

HONORABLE JACOB HART
UNITED STATES MAGISTRATE JUDGE